(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 957 651 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
17.11.1999 Bulletin 1999/46

(51) Int Cl.[6]: **H04Q 7/32**

(21) Application number: **99850079.7**

(22) Date of filing: **10.05.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **12.05.1998 SE 9801635**

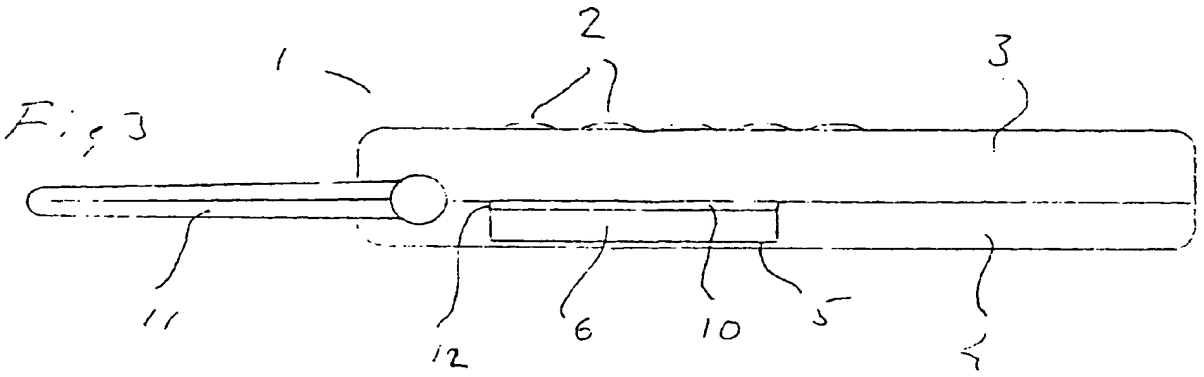
(71) Applicant: **Sectra Communications AB**
583 30 Linköping (SE)

(72) Inventor: **Mastrovito, Eduardo**
586 66 Linköping (SE)

(74) Representative: **Berglund, Erik Wilhelm**
Berglunds Patentbyra AB
Aspebraten
590 55 Sturefors (SE)

(54) Mobile telephone with cypher card

(57) Mobile telephone (1), for instance a GSM telephone with a corresponding SIM card (8) for authentication within a GSM network. The telephone is additionally provided with a reception slot (12) for a smart card (10) containing ciphering keys that on temporary insertion together with additional enciphering and deciphering circuits and programs in the telephone can make very secure end to end communication possible. In this way eavesdropping or accidental overhearing becomes practically impossible.



BEST AVAILABLE COPY

EP 0 957 651 A2

3NSDOCID: <EP_____0957651A2_I_>

Description

[0001] Today a substantial portion of all telephone communications is done over mobile telephones instead of fixed telephones. Since mobile communications includes radio transmission it has at the same time become easier to eavesdrop a telephone conversation, in particular in the case of cordless telephones. Even if uplink and downlink as in the GSM case are separated in frequency and time, and the amount of possible frequencies is large, intelligent scanning devices can fairly easily succeed in tracking a particular conversation and eavesdrop. Sometimes it may of course also be sufficient to hear the communication in one direction to gain valuable understanding of the ongoing conversation. In the old days of fixed communications one had to tap the wireline to eavesdrop a conversation, this in turn being detectable and punishable. With mobile phones the eavesdropping can be done in complete secrecy and without detection risk so although still illegal, it can not really be stopped. The ciphering of the radio links optionally applied in GSM and DECT systems can make eavesdropping more difficult but still feasible due to the relative weakness of the GSM and DECT ciphers. A conversation could be recorded, analyzed and deciphered offline.

[0002] Furthermore all mobile communications must be routed as plain speech or binary data streams through at least some parts of the mobile network's fixed infrastructure (e.g. base stations, base station controllers and mobile switching centers). It is thus also possible to eavesdrop a mobile telephone by tapping some wires in e.g. a base station.

[0003] There is also the risk that conversations are overheard by chance. This is even more likely to occur with so-called cordless telephones since these share a smaller amount of frequencies.

[0004] At the same time an increasing amount of data such as agreements, business information, technical information and other confidential information is communicated over the telephone networks, in particular over mobile telephone networks.

[0005] In view of the above problems it is the object of the invention to enable a more secure transfer of confidential information via mobile telephones, cordless phones and the like radio based communication devices or equipments.

[0006] The object of the invention is solved by the invention by providing the telephone with additional ciphering means including a connection for an additional smart card containing the ciphering keys. This enciphering smart card, hereinafter abbreviated ESC, includes memory means and/or processing means, and can enable enciphering of the speech in a preprogrammed way which only a corresponding ESC in the receiving telephone is aware of. Only the ESC in the intended receiver (s) is provided with the same cipher keys as the originator.

[0007] The additional chipering is performed end to end which means that the enciphered message is protected all the way from originator to recipient preventing thus eavesdropping along the transmission path - including fixed network elements such as base stations.

[0008] Instead of providing only the enciphering keys the ESC could take care of the entire ciphering function.

[0009] Since most mobile phones are already equipped with a smart card (SIM card) for various identification purposes, most telephones according to the invention will be provided with two cards with different contents, and different objects as well as different locations in the phone. The SIM card remains normally in the phone and may therefore be situated e.g. behind the battery pack. The ESC however is to be insertable and removable with ease during operation.

[0010] Also cordless telephones could be provided with an ESC.

[0011] It needs not only be the case of two telephones that can communicate in this way, instead it could be a group of telephones, in which case a number of ESCs are configured to co-operate.

[0012] In a further development of the invention a group of ESCs may be organized in different levels or in a different way so that for instance a master ESC can enable contact with all ESCs in the group whereas the other ESCs may be divided into subgroups that can only communicate within the subgroup and with the master ESC telephone. In other words the ESC hierarchy can be designed to match very specific needs.

[0013] Since a telephone with an ESC in it can be stolen or lost it is suggested in accordance with a further development of the invention that the ESC is easy to remove from the telephone at any time. Indeed it is preferable that the telephone cannot be returned to its idle state without the removal of the card. In the case of a foldable phone where for instance the mouthpiece is folded as a lid over the keyboard, folding may be prevented mechanically by the card itself, it may for instance when inserted extend into the path of the lid. The insertion of the card can alternatively trigger a simple mechanical device locking the lid in its open position. In this way it is difficult to forget removing the ESC. The telephone may also signal or warn that the card is in the phone if one tries to close the lid or to shut it off with the ESC still in it.

[0014] Instead of having an elaborated hierarchy among the ESCs, users may possess a number of ESCs for different communication paths or different persons that they wish to communicate in secrecy with. Also it is not necessary that all ESCs are intended for speech communication. Since an increasing portion of all mobile communications consists of data it is easily foreseen that the invention will be used for data communications as well. Banking services are an example of data services that require confidentiality.

[0015] Although the telephone according to the invention may be of any type it may in particular be:

EPNSDOCID: <EP_____0957651A2_I_>

a GSM900 mobile station,
a DECT portable part
a dual-mode GSM900/DECT terminal
a dual-band GSM900/DCS1800 terminal
a triple-band GSM900/DCS1800/PCS1900 terminal
a TETRA mobile station
a UMTS mobile station
a dual-mode GSM900/UMTS terminal
a dual-mode GSM900/Satellite terminal

[0016] In some of these cases the telephone will in addition to the ESC be equipped with two other cards for the networks' identification and authentication.

[0017] Further preferable developments of the invention are apparent from the claims and the following description of a preferred embodiment shown in the drawings. In the drawings fig 1 shows a mobile telephone according to the invention in a lateral view in a first position, fig 2 the same phone in a second position and fig 3 the phone in a third position.

[0018] The telephone 1 in the drawings is provided with keys 2 and a display (not visible) Between the top 3 and bottom 4 shell of the telephone housing an opening 5 is present for the insertion of a flat battery 6. When the battery is removed a small receptacle 7 for a SIM card 8 tilts up into the battery opening and the SIM card is accessible for removal or insertion through the slot or opening 5 as can be seen in fig 2. When the battery is once again inserted the receptacle tilts back out of the way.

[0019] Next to the battery slot 5 above and adjoining this is an opening slot 12 situated so that the total opening is about two millimeter wider than the battery thickness requires. Into this slot 12 an enciphering smart card (ESC) for end to end encryption can be inserted. This card has the the size of a credit card. When this card is inserted its contact points are contacted by the contacts 9 shown next to the SIM-card receptacle 10. The ESC can not be inserted in its entirety into the phone but will when inserted to its working position still extend outside the housing by about one half, making it practically impossible to forget it there after use.

[0020] The ESC can be inserted before a communication is commenced or during communication.

[0021] The telephone is in its lower end provided with an antenna 11 that is mounted for a swing movement parallel to the length direction of the phone, from the position shown in fig 1 to the position in fig 2. The antenna is resiliently pretensioned towards the body of the phone snap locking it in its folded or rest position along the side of the phone covering the ESC slot, thus preventing the introduction of unintended objects as long as the antenna is in rest position. In this way the user will also find it impossible to fold the antenna if the ESC remains in the phone.

[0022] The resilient mounting of the antenna result not only in snap locking it but will also protect the mounting from being accidentally damaged.

[0023] The antenna may be provided with snap-lock means enabling locking of a position obliquely backwards so that the telephone can stand up on a table.

[0024] In a slightly altered version the antenna may be slidably extendable downwards and at the same time serve as a lid over the ESC slot. Also a connection for an external antenna may be arranged together with other connections in a known manner.

[0025] The ESC may also include pin codes or other choices made by the user, for instance depending on whom he intends to contact. The ESC may also contain the telephone number of the receiver. The ESC may also be tightly bound to a specific telephone so that it can not be used unless one has access to the intended telephone.

Claims

1. Radiobased communication device or equipment for instance telephone **characterized in** being equipped with an enciphering circuit operating end to end and receiving the cipher keys from a cipher smart card that is insertable into an apposite slot in the telephone so as to enable enciphering or deciphering of speech and/or data to and from the telephone.

2. Device according to claim 1 in particular a mobile telephone **characterized in** that it is also equipped with a communication smart card for mutual identification and authentication between the device and the network service provider.

3. Device according to claim 1 or 2, **characterized in** the slot in the device for the accommodation of the cipher smart card being so located that the mouthpiece or keyboard lid can not be folded without the removal of the card.

4. Device according to any of the preceding claims, **characterized in** the enciphering circuit being contained in the cipher smart card.

5. Device according to any of the preceding claims, **characterized in** transmitting speech over any of the data channels of the GSM-system.

6. Device according to any of the preceding claims, **characterized in** being equipped with more than one slot or location for smart cards for instance so that two or more persons must insert their cards to enable ciphered communication.

7. Device according to any of the preceding claims, **characterized in** being a GSM900 mobile station or a DECT portable part.

ENSDOCID: <EP_____0957651A2_I_>

8. Device according to any of the preceding claims, **characterized in** being a multiple mode telephone, for instance a dual-mode GSM900/DECT terminal, a dual-band GSM900/DCS1800 terminal, a triple-band GSM900/DCS1800/PCS1900 terminal, a dual-mode, GSM900/UMTS terminal or a dual-mode GSM900/Satellite terminal.

9. Device according to any of the preceding claims, **characterized in** being a TETRA mobile station, or a UMTS mobile station.

10. Device according to any of the preceding claims, **characterized in** the cipher smart card not being fully insertable rendering it less easy to be unintentionally left in the device, for instance a telephone.

11. Device according to any of the preceding claims **characterized in** an antenna that is foldable or retractable and also covering or closing the cipher smart card slot or opening when folded along the device and in particular telephone body.

BNSDOCID: <EP_____0957651A2_I_>

Fig 1

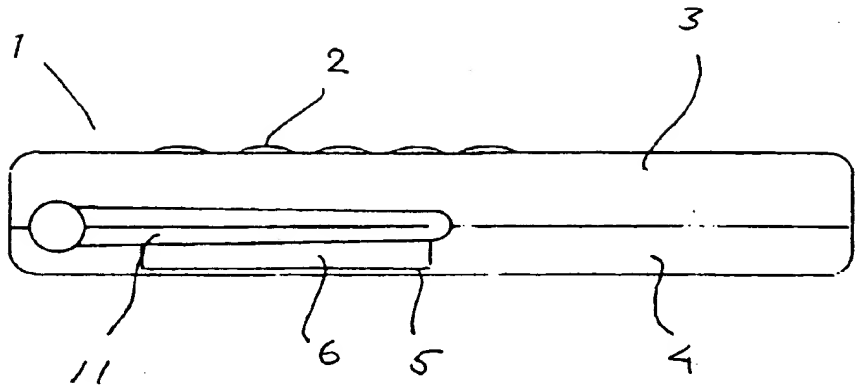


Fig 2

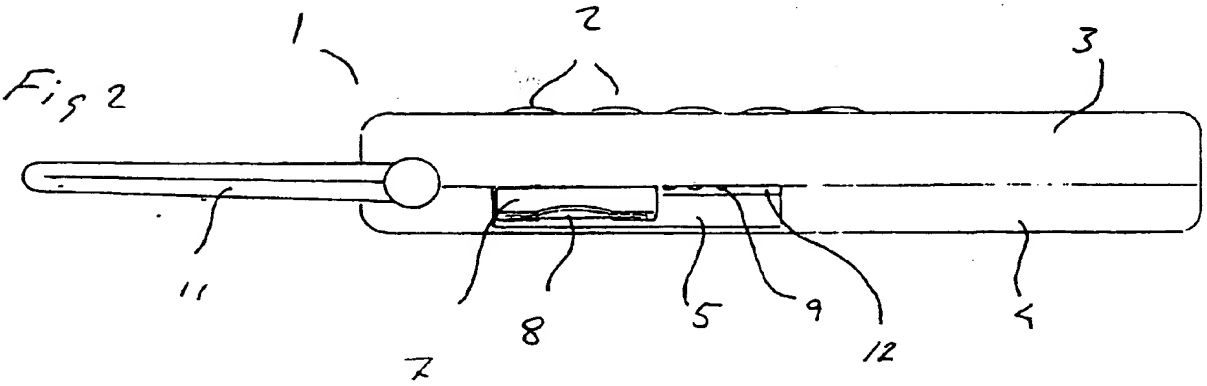
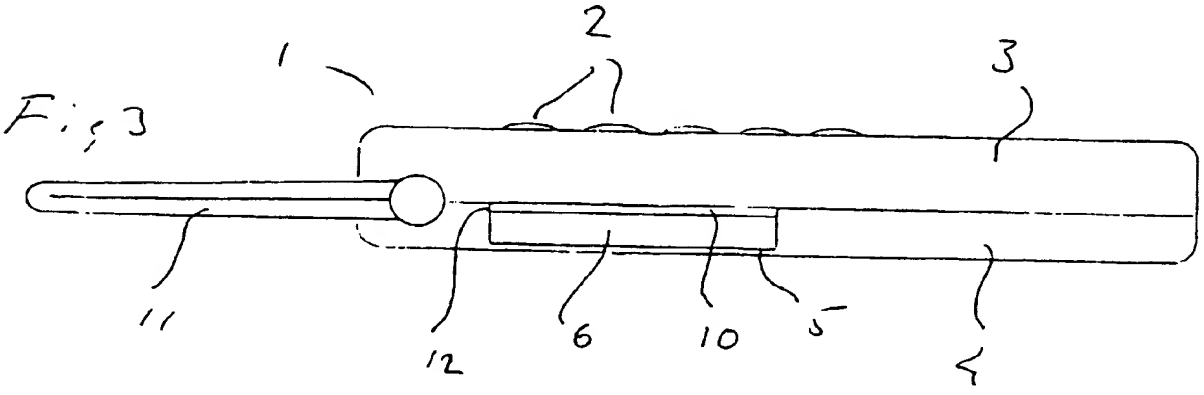


Fig 3



BEST AVAILABLE COPY

BNSDOCID: <EP_____0957651A2_I_>

THIS PAGE BLANK (USPTO)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 957 651 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
06.09.2000 Bulletin 2000/36

(43) Date of publication A2:
17.11.1999 Bulletin 1999/46

(51) Int Cl.[7]: **H04Q 7/32**

(21) Application number: **99850079.7**

(22) Date of filing: **10.05.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **12.05.1998 SE 9801635**

(71) Applicant: **Sectra Communications AB**
583 30 Linköping (SE)

(72) Inventor: **Mastrovito, Edoardo**
586 66 Linköping (SE)

(74) Representative: **Berglund, Erik Wilhelm**
Berglunds Patentbyra AB
Aspebraten
590 55 Sturefors (SE)

(54) Mobile telephone with cypher card

(57) Mobile telephone (1), for instance a GSM telephone with a corresponding SIM card (8) for authentication within a GSM network. The telephone is additionally provided with a reception slot (12) for a smart card (10) containing ciphering keys that on temporary insertion together with additional enciphering and deciphering circuits and programs in the telephone can make very secure end to end communication possible. In this way eavesdropping or accidental overhearing becomes practically impossible.

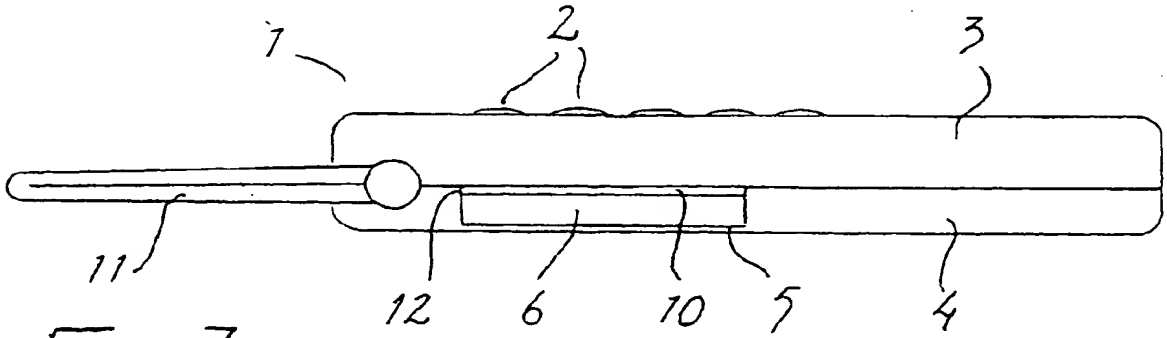


Fig.3

BEST AVAILABLE COPY

EP 0 957 651 A3

BNSDOCID: <EP_____0957651A3_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 85 0079

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	VAN BOSCH J: "CREDIT-CARD ENCRYPTION WITH KEY STORAGE" MOTOROLA TECHNICAL DEVELOPMENTS,US,MOTOROLA INC. SCHAUMBURG, ILLINOIS, vol. 15, 1 May 1992 (1992-05-01), pages 21-22, XP000305724 * the whole document * ---	1,2,4,5, 7,9	H04Q7/32
X	COOKE J C ET AL: "THE USE OF SMART CARDS IN PERSONAL COMMUNICATION SYSTEMS SECURITY" PROCEEDINGS OF THE CONFERENCE ON TELECOMMUNICATIONS,GB,LONDON, IEE, vol. CONF. 4, 1993, pages 246-251, XP000473732 * page 249, left-hand column, line 24-37 * ---	1,2,4,5, 7,9	
P,X	DE 197 07 022 A (SIEMENS AG) 27 August 1998 (1998-08-27) * the whole document * ---	1,2,4,5, 7,9	
A	US 5 485 519 A (WEISS KENNETH P) 16 January 1996 (1996-01-16) * column 1, line 24 - column 3, line 27 * * column 7, line 32-63 * * column 12, line 16-29 * -----	1,2,4,5, 7,9	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04Q

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
THE HAGUE	2 March 2000	Weinmiller, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____0957651A3_I_>

European Patent Office

Application Number
EP 99 85 0079

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

1,2,4,5,6,7,8,9

BNSDOCID: <EP_____0957651A3_I_>

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 99 85 0079

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1,2,4,5,6,7,8,9

in a cellular telephone a card is provided storing/generating the keys needed for end-to-end encryption of communication; encryption circuit may also be on this card; possibly this is a second card besides the SIM card for authorisation; solves the problem of providing keys for encryption and encryption engine in a mobile phone

2. Claims: 3,10,11

constructional features to prevent forgetting a smart card in the mobile telephone after use if it is desirable to not let it there;

3NSDOCID: <EP_____0957651A3_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 85 0079

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

02-03-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19707022 A	27-08-1998	NONE	
US 5485519 A	16-01-1996	US 5367572 A	22-11-1994
		US 5237614 A	17-08-1993
		US 5657388 A	12-08-1997
		US 5479512 A	26-12-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____0957651A3_I_>

THIS PAGE BLANK (USPTO)